AIRPORT COOPERATIVE RESEARCH PROGRAM

Research Results Digest 11

Helping Airports Understand the Payment Card Industry Data Security Standard (PCI DSS)

DETAILS

29 pages | | PAPERBACK
ISBN 978-0-309-15502-1 | DOI 10.17226/14436

AUTHORS

October 2010

AIRPORT COOPERATIVE RESEARCH PROGRAM
Sponsored by the Federal Aviation Administration

Responsible Senior Program Officer: Theresia H. Schatz

Research Results Digest 11

HELPING AIRPORTS UNDERSTAND THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

This digest presents the results of ACRP Project 11-02/Task 14, "Helping Airports Understand the Payment Card Industry Data Security Standard" and its applicability to the airport environment to help ensure that airport business systems meet this commercial standard. The research was conducted by Rick Belliotti and David Jividen of Barich, Inc., Chandler, Arizona.

CONTENTS

BACKGROUND

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements for ensuring protection and security of credit cardholder data. The standard was developed by American Express (AMEX), Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International to facilitate the adoption of a consistent data security program on a global basis. The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design, and other protective measures.

The PCI DSS has become a major topic for airports and airlines as they attempt to determine how this standard affects them and which elements of the standard apply to their organization. In addition to PCI DSS, the PCI has also created the Payment Application Data Security Standard (PA DSS), which defines how software vendors and others develop secure payment applications. The PA DSS applies to payment application software developed for the purpose of sale and distribution. For payment applications that are developed in-house, for the sole use of the business or organization, the PA DSS does not apply because security is covered in the PCI DSS compliance program. To learn more about the PA DSS and the restrictions therein, the PCI Security Standards Council (PCI-Council) has created a webpage and documents describing these requirements (*1*). The third standard that exists for PCI security is the PCI personal identification number (PIN) transaction Security (PCI PTS) standard. This standard is focused on protecting transactions that involve PIN numbers. See Figure 1 for a diagram of the relationships between these standards.

The entire PCI DSS presents some ambiguity not only to all businesses and organizations employing the use of payment cards, but also particularly to airports and the business of airport operations. Airports present a unique situation in which airport systems and infrastructure must connect and operate with the following:

- Airline tenants using gates and ticket counters and, thus, airport networks at a minimum;
- Self-service kiosks for passenger processing;
- Common use equipment used by multiple airlines/merchants;
- Airport business tenants using space (and possibly airport services) in airport terminals for retail, service, and restaurant businesses;

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

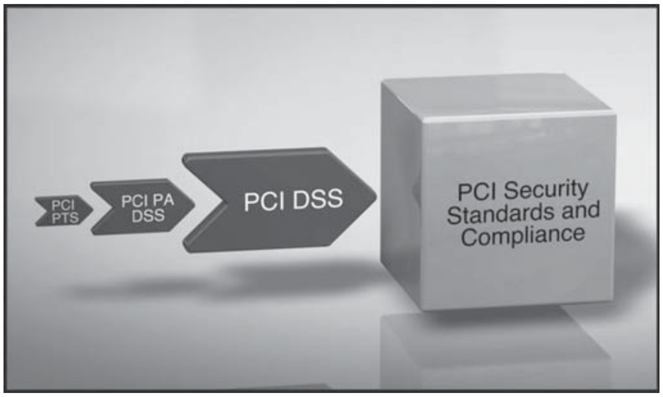


Figure 1 PCI standards relationships.

- Third-party software potentially used for delivering and receiving airline information, managing airport resources, and supplying passenger-facing information;
- Third-party service providers used for conducting airport processes and/or supplying resources; and
- Business processes for regular accounting functions (receivables, payables, etc.).

These factors present an airport with a myriad of possible conditions for which it may or may not need to consider PCI DSS compliance as a necessity. Additionally, with potential variations in the interpretation of compliance validation requirements, airport management faces a “where do I start?” and “where am I going?” situation.

The research conducted for this project found that card brands consider PCI DSS requirements as applicable to all businesses or organizations that conduct business using payment cards or cardholder data in their process(es). There is not a specific airport-centric compliance perspective in the PCI; however, qualified security assessors (QSAs) or PCI consultants and auditors would be able to apply PCI DSS requirements to airport-specific conditions.

Airports do not present a “one size fits all” opportunity when it comes to PCI DSS compliance. The various airport sizes and configurations, number of tenants, contractual arrangements, government organization and authority set up, transaction volumes, network segmentation, and classification (merchant, service provider, or both), generate a complex set of scenarios, each one needing a unique PCI program that will meet the compliance objectives. An airport may be a merchant, accepting credit card transactions and/or be a service provider, providing network services to its business tenants and air carriers.

The time investment made by airports that have either started or are already engaged in their PCI compliance program appears to be widely varied due to the complexities just described. In any of the cases, the investment is considerable and should not be estimated in weeks, but rather in months to years depending on the tasks that are required for completion. Airports may consider starting with the self-assessment questionnaire (SAQ), available through the PCI-Council or through the various QSA consulting firms.

PURPOSE

The Transportation Research Board commissioned this quick response project because of the need to provide background information on the data protection requirements for the PCI DSS and its applicability to the airport environment. As such, this document presents the PCI DSS and the impacts that an airport needs to consider when reviewing their credit data retention policies and systems that process credit card payment transactions.

Airports today are assuming more responsibility and direct ownership of information systems that accept credit card payments. These payments include parking revenue, concession sales, and other services. Airports are being classified by the PCI as merchants and service providers, depending on the level and types of transactions they are supporting. Because of these classifications, the airport operators are required to undergo PCI DSS audits to ensure that they have the proper protections and systems in place to protect cardholder data.

A guide is needed by airports to help them understand the data and network protection responsibilities they must assume when accepting card transactions. The objective of this report is to present an analysis of the PCI DSS, to give an overview of the systems that may be affected, and to present areas for further research and study. The result is an introductory guide for airports as to their responsibilities associated with the commercial PCI DSS.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Basics of the PCI DSS

PCI Security Standards Council

The PCI DSS is a set of standards, developed by the PCI-Council, for the purpose of ensuring payment card data/information security.

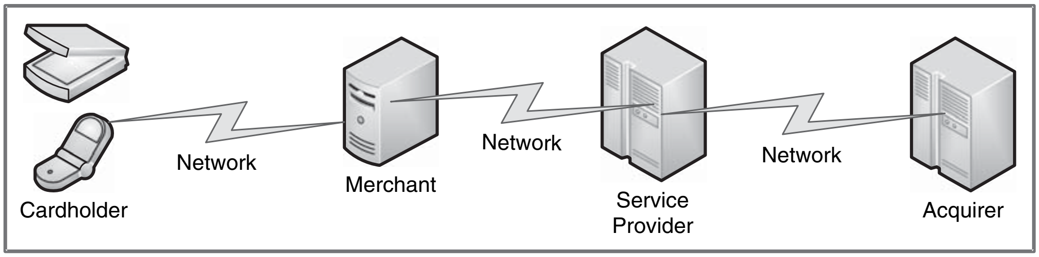


Figure 2 PCI process entities.

The PCI-Council is an organization founded by the major payment card brands—Visa Inc., MasterCard Worldwide, American Express, Discover Financial Services, and JCB International*—in collaboration, to provide direction, guidance, and standards to protect cardholder data information that is subjected to the various methods and mechanisms of transaction processes. While the PCI-Council is responsible for all aspects of PCI standards, it does receive input from an advisory board made up of participating organizations engaged in various aspects of the PCI. The PCI-Council has also implemented certification programs for QSAs and Approved Scanning Vendors (ASVs), creating a mechanism to produce qualified resources to help businesses assess and meet PCI compliance standards.

Basic PCI Process

The flow of a payment card transaction engages multiple entities and, therefore, the data/information included in a transaction is also transmitted through several points of control. The components and/or entities involved include the following:

- Cardholder—authorized payment card user;
- Issuer—financial institution that issues payment cards and maintains a contract with cardholders for repayment;
- Merchant—authorized acceptor of payment cards for the payment of goods and/or services;
- Acquirer—financial institution or merchant bank that contracts with the merchant for payment card acceptance and enables payment card payments from customers;
- Consumer Payment Card (brand or system)—financial institution that issues payment cards and/or signs merchants to accept payment cards (Visa, MasterCard, AMEX, Discover, and JCB); and
- Payment Network—network accessed through a service provider that acts as the authorized communication vehicle for transmitting the payment card transaction and for handling the transfer of payment transactions between parties.

These relationships, and the basic places in the payment process in which they apply, are shown in Figure 2.

There are two main phases for processing a payment card transaction, as shown in Figure 3. Authorization (Phase I) is the transaction, or request, that is initiated electronically when an approval or rejection decision is made by the appropriate authorization issuer. Upon approval, Phase II, clearing and settlement, is initiated when accounts are debited/credited according to the transaction amount (*2*).

PCI Environment

There are three sets of standards covering the different aspects of the PCI transaction environment:

1. Businesses that use payment cards as a means of payment for services or products,
2. Card device manufactures, and
3. Payment card application development.

Airport businesses would fall into the first category of standards, the DSS that has been established as a common set of requirements to protect cardholder data when transactions involve technological means to complete the process described above. At any point in business operations in which cardholder data is stored (either electronically or in a hardcopy format) and is used in a payment process (electronic transmission of the data), the business is required to abide

* The Transportation Research Board, the National Research Council, and the Federal Aviation Administration (sponsor of the Airport Cooperative Research Program) do not endorse products or manufacturers. Trade or manufacturers names appear herein solely because they are considered essential to the clarity and completeness of the project reporting.

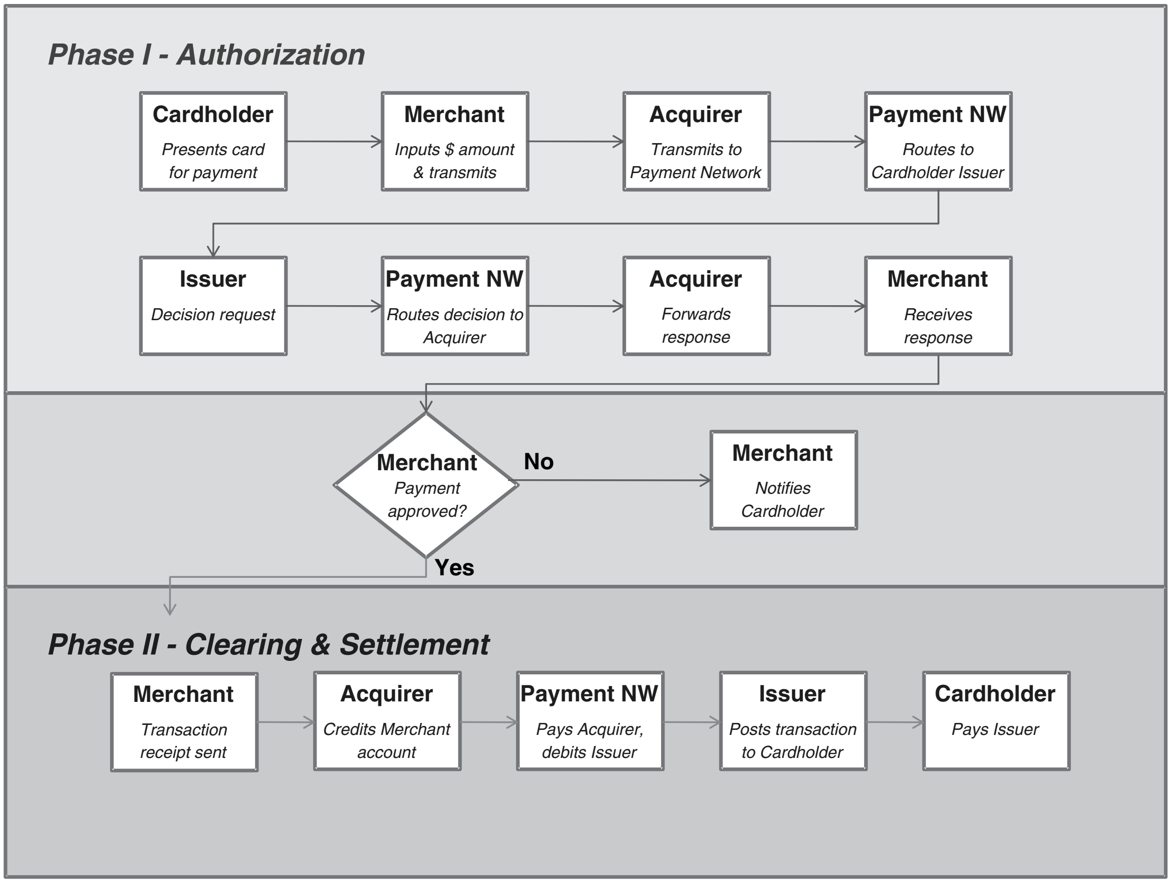


Figure 3 Payment card transaction process flow.

by the PCI DSS. An airport may operate as multiple roles within the PCI environment. They may act as a merchant by accepting payment cards to receive payment and/or as a service provider when their network or applications are utilized for the purpose of storing, processing, or transmitting cardholder data, while not being the receiver of payment for goods or services. According to the *PCI Compliance Guide,* for the purpose of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of the PCI-Council as payment for goods and/or services (*3*). And a service provider is any company that stores, processes, or transmits cardholder data on behalf of another entity (*4*).

PCI DSS Risks

The process of a merchant or service provider receiving cardholder data and then using it for processing or transmitting from a local network to a gateway or external network has the potential for a data security breach or an exposing of vulnerable points from which data could be intercepted intentionally or unintentionally. Either way, data security is expected and required through the requirements set forth by the DSS.

Vulnerable points of an airport business would include:

- Self-service kiosks where a payment card is used to identify the cardholder and/or to process a payment;
- Other payment stations where payment card data is collected;
- PIN entry devices;
- Networks and network connection points;
- Wi-Fi access points;
- Airport application systems, including:
  - Databases storing cardholder data and redundant systems for business continuity;
  - Application processing and interfaces between systems; and
  - Access, security, authorization, and administration of systems connected to cardholder data;

- System reporting, exposure of cardholder data visibility on reports; and
- Cardholder data handwritten or printed and stored in a non-electronic repository.

While there are many more areas of vulnerability or exposure, the PCI DSS provides a method to ensure that the technology incorporated by the airport has been investigated, compared, and remediated if necessary to meet the requirements of the standard and that a process is in place to maintain the standard and to manage the introduction of changes in systems and technology.

The impact of a cardholder data breach goes far beyond any fines or penalties that may be incurred. The immediate impact of correcting the situation would involve costs for fixing, testing, and implementing as well as a possible shutdown of functionality during the remediation process. Additionally, there is the cost to identify, notify, and provide recommended actions for affected customers/cardholders to take. The potential costs for legal fees would exist should individual or class-action lawsuits be initiated. And the loss of confidence of customers or of employees could generate impacts that are not easily measured in dollars. There have been numerous examples of these types of breaches in the recent past that demonstrate the cost and impact of a cardholder data breach.

PCI DSS Compliance

PCI DSS compliance is expected of all organizations utilizing cardholder data. The PCI DSS comprises 12 basic requirements within six categories of objectives that must be met. An organization using a payment card of any of the card brands to conduct business operations must provide evidence, through the validation requirements, that PCI DSS compliance has been met. The validation requirements are based on varying situations. The card brand, the operation of the organization (merchant or service provider), and the volume of transactions or other conditions make up the factors involved in determining the level of the organization or business. The levels and corresponding compliance assessments or validation methods will be discussed in more detail later in this document. The PCI DSS requirements are expected to be met as a standard throughout the industry although each card brand defines its own business-level definitions along with its own validation requirements. It is this individuality between the card brands that causes the most confusion when attempting to understand the PCI DSS.

The card brands themselves enforce compliance through a set of compliance validation requirements that are defined for each level established by the card brands. Each level will have a series of tests, audits, and assessments that must be validated by the defined qualified resources required by the card brands. In addition to the validation requirements, the card brands set, or will set, deadlines for meeting the validation requirements. These deadlines may be applied to the compliance requirements in general or possibly to an individual validation requirement.

Airport Functions Affected by the PCI DSS

What does this mean for the various managers in the airport business operation? While there is definitely a technology-centric perspective to PCI DSS compliance, the responsibilities and potential impact may be felt in many functional areas. Each of the management roles listed below may be conducted in various ways depending on the airport size and organization structure, including as outsourced functions. It will be up to each airport to determine the actual impact to their respective areas of responsibility.

Airport Executives

In the research conducted with airports, there seems to be no lack of understanding by airport executives as to the potential risks of non-compliance and the urgency to address those risks. However, the investment in time and money required to achieve compliance is a concern. This is especially the case where auditors vary in the interpretation of the requirements and may make compliance and validation a higher contributor to both cost and time.

Airport executives must consider not only the impact of non-compliance and the associated risks, but also that an ongoing program requires continued support and communication of the importance to all levels of staff and airport employees on a frequent basis. A change in culture in any business is difficult and this is no different for an airport. The assignment of airport executives for compliance responsibilities ensures that a focal point with full authority is communicated throughout the organization. Regular executive staff meetings should include an agenda item on compliance progress and ongoing compliance reports. Visibility of updated compliance metrics (exposures, breaches, recoveries, etc.) ensures an ongoing focus on data security and on the needed awareness of its importance to the airport staff.

Technology Division

As previously stated, PCI DSS compliance has a focus on technology. The technology division will be heavily involved in the program from development through implementation and continued oversight. The information needed to prepare for the PCI DSS will be based in the technology division. It is here that the initial assessment will be formulated and the data collected on existing databases, applications, networks, transaction volumes, transaction data, encryption technology, gateways, and so on.

The technology division will have primary input into technical challenges that will need to be overcome and into the cost in resources and infrastructure that may be required to achieve compliance. The roadmap or program plan will be constructed by the technology division to provide a strategy for prioritization of tasks, resource consumption, cost estimates, schedules and phases, and the methods for moving from the existing environment to a compliant environment.

The technology division will also be required to develop the approach for the actual audit and validation sessions. They will need to investigate any airport operator perspectives on finding the appropriate QSA vendor or ASV depending on the level and requirement validation necessary. The technology division will ensure that audit planning and preparation is complete and ready to engage. Key points of preparation include:

- Readiness of documents;
- Required samplings and test preparation;
- Test resources;
- Staff assigned, aware, and prepared for working with auditors;
- Introductory session with auditors including contact information; and
- Documents organized and appropriate authorization established for auditor access.

The technology division should be in constant communication with the PCI DSS compliance officer assigned by the airport executive management during the audit preparation time and should provide progress reports during the actual audit time period.

Aviation Administration

The aviation administration will be responsible for assessing current processes (system and/or manual) engaging cardholder data, in both electronic and hard-copy formats. The aviation administration will need to conduct an asset inventory of file cabinets, desks, secured rooms, and access authorization processes for any non-electronic security of cardholder information. This may require process review of room/file cabinet key distribution, key cards for room access, and returns due to employee termination.

The aviation administration will need to work closely with the technology division to modify and implement process changes or new process introductions in order to achieve compliance acceptance.

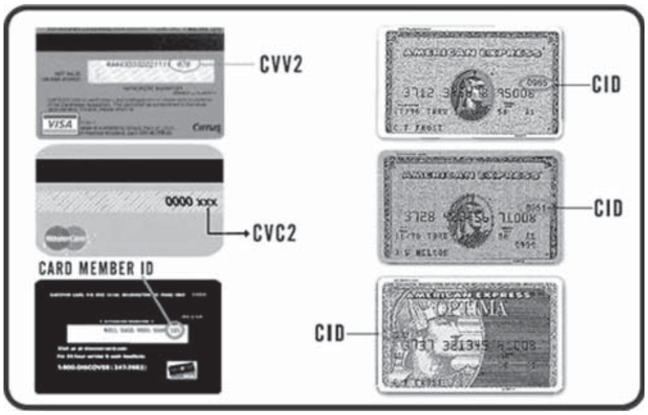
Fiscal Division

The fiscal division is also a key stakeholder in PCI DSS compliance. Financial processes require strict adherence to secure processes for which cardholder data is in use. The fiscal division will also work closely with the information technology (IT) manager dealing with such financial processes both in assessing current practices and required changes. Point of sale (POS) processes will definitely be susceptible to vulnerabilities, and a thorough understanding of how data is used, processed, and transmitted will be required.

Internal financial processes such as reconciliation, irregular conditions, scheduling and timing, data security methods (lock box, third-party service, etc.) will need to be addressed as a part of a PCI DSS program.

Business and Properties Division

The business and properties division will benefit from engagement with the airport PCI DSS compliance program by recognizing contractual details that should be included in renting or leasing airport space to ensure that tenants and the airport have a thorough understanding of the security permissions and requirements. The data collected and used in this functional area would need to be investigated to ascertain if there are any cardholder data touch-points or vulnerabilities that need to be addressed.



Note: CVV2 = card authentication value 2 (Visa), CID = card identification number (AMEX and Discover), and CVC2 = card validation code 2 (MasterCard).

Figure 4 Card verification value locations.

Risk Management and Legal

While risk management and legal are two separate entities that may exist within an airport organization, they may be outsourced functions as well. The importance of these functions working closely together to ensure PCI DSS compliance is considered in preparing contracts and in managing liability and insurance perspectives.

The risk management role generally concentrates on costs and loss potentials. The consideration that PCI DSS non-compliance or security breaches can impact the airport with significant fees, penalties, and recovery costs provides an incentive for this role to engage in the PCI DSS program.

PCI COMPLIANCE

Compliance Requirements

Payment Card and Data

The International Organization for Standardization (ISO) presents the standards for the characteristics of payment cards, including the physical size, how they are to be embossed, the characteristics of the magnetic stripe, and the location of the tracks of data included on the magnetic stripe.

Printed on the card, but not included in the encoded data, is a Card Verification Value (CVV) (see Figure 4). The printed code (not embossed) is defined differently by the card brands, and is possibly printed in different locations. AMEX prints a four-digit code on the front of the card while the other card brands print the code on the signature side (magnetic stripe side) of the card.

The magnetic stripe contains up to three tracks of encoded data.

- Track 1 was developed by the International Air Transportation Association (IATA) for intended use in the airline industry for ticketing and reservations.
- Track 2 was developed by the American Bankers Association (ABA) for the intended use of payment cards for financial transactions.
- Track 3 was developed by the thrift industry and is not commonly used and sometimes is not even present on the magnetic stripe.

Table 1 identifies the key data elements encoded within each track.

Table 1 General magnetic stripe track data.

Track	No. of Characters	Character Type	Element 1	Element 2	Element 3	Element 4
1	79	Alphanumeric	Primary Account No. (PAN) (19)	Name (26)	Additional Data (Expiration Date (4)/Service Code (3))	Discretionary Data (Card Brand discretion)
2	40	Numeric	PAN (19)	Additional Data (Expiration Date (4)/Service Code (3))	Discretionary Data (Card Brand discretion)	
3	107	Numeric	PAN (19)	Additional Data (17 fields, some optional)	Discretionary Data (5 fields, some optional)	

NOTE: The table does not include the "start and end sentinels," "field separators," "format code," or "longitudinal redundancy check character." The numbers in parentheses indicate the maximum number of characters for the element.

A more detailed chart of the magnetic stripe track data elements is available in Appendix A of this document. The discretionary data varies by card brand and what is included is optional. The data may include a PIN verification key indicator (PVKI), PIN verification value (PVV), CVV, or card verification code (CVC) (*5*).

Not all data available on the payment card data track is permitted to be stored in a local database (see Objective 2, Requirement 3 in the Requirements section below). Only the primary account number (PAN), the cardholder name, the service code, and the expiration date are eligible for storage. None of the discretionary data, including the validation or verification codes, PIN, or PIN block should be included in the electronic storage of cardholder data. Additionally, where the PAN is displayed in a visible format, it should be masked so that only the first six digits and/or the last four digits are identifiable (*6*).

PCI DSS Requirements

The PCI DSS is established as a set of objectives and requirements for any organization using payment card(s) or cardholder information to conduct business operations. The requirements are not just simple guidelines but are a mandatory set of expected methods and processes that not only must be operational, but also validated as operational in the business. The PCI-Council defines cardholder data as the full magnetic stripe (which cannot be stored) or the PAN plus any of the following:

- Cardholder name,
- Expiration date, and
- Service code. (*7*)

There are six objectives of the PCI DSS:

1. Build and maintain a secure network,
2. Protect cardholder data,
3. Maintain a vulnerability management program,
4. Implement strong access control measures,
5. Regularly monitor and test networks, and
6. Maintain an information security policy.

Each of these objectives includes a set of requirements that, when implemented, enables the business or organization to meet the objective and comply with payment card information security. The following list of requirements includes further explanation from PCI experts as a part of an interview process conducted by the research team, and, where provided, includes any specific comments related to airports.

Objective 1: Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

- Maintain up-to-date diagrams of all current networks with all connections to cardholder data including any wireless networks.
- Ensure that each Internet connection has a firewall.
- Establish a formal process for approving and testing all network connections and changes to the firewall and router configurations.
- Document explanation of groups, roles, and responsibilities for logical management of networks and network components.
- Review firewall and router rule sets on a frequent basis (at least every 6 months).
- Restrict firewall configuration connection between entrusted networks and any system components in the cardholder data environment.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Objective 2: Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

- Use strong cryptography and security protocols such as secure socket layer (SSL) and transport layer security (TLS) or Internet Protocol Security (IPSEC) during transmission over open networks.
- Use strong encryption for authentication and transmission on wireless networks that transmit cardholder data or connect to the cardholder data environment.
- Never send unencrypted PAN by end-user messaging technologies (email, instant messaging, or chat).

Objective 3: Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software.

- Deploy anti-virus software on all systems.
- Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

- Ensure that all anti-virus mechanisms are current, active, and generate audit logs.

Requirement 6: Develop and maintain secure systems and applications.

- Ensure all system components and software have the latest vendor-supplied security patches (applicable to purchased software) installed.
- Establish a process to identify newly discovered security vulnerabilities.
- Have in place and follow change control procedures for all changes to system components, including:
  - documentation of impact,
  - management sign-off by appropriate parties,
  - test operational functionality, and
  - back-out procedures.

Objective 4: Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know.

- Limit access to system components and cardholder data to only those individuals whose jobs require such access.

Requirement 8: Assign a unique ID to each person with computer access.

- Assign a unique username/password before allowing them to access system components or cardholder data.

Requirement 9: Restrict physical access to cardholder data.

- Shred, incinerate, or pulp hardcopy cardholder data.
- Render electronic cardholder data unrecoverable.
- Monitor physical locations of cardholder data environments and limit access to only individuals with access privileges—use of video cameras and access control mechanisms.
- Restrict physical access to wireless access points, gateways, and handheld devices.
- Store media back-ups in a secure location, preferably an off-site facility such as an alternate or back-up site or commercial storage facility (include security review at least on an annual basis).
- Physically secure paper and electronic media that contain cardholder data.

Objective 5: Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

- Establish a process for linking all access to system components to each individual user.
- Synchronize all critical system clocks and times.
- Review system components logs daily.
- Secure audit trails to prevent tampering:
  - limit visibility of audit trails to those with a job-related need,
  - protect audit trail files from unauthorized modifications,
  - back up audit trail files to a centralized log server or media difficult to alter,
  - use file integrity monitoring or change detection software on logs to generate alerts for any data changes.

Requirement 11: Regularly test security systems and processes.

Objective 6: Maintain A Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

- Implement and maintain policies and procedures to manage service providers if the airport shares cardholder data with service providers.
- Establish, publish, maintain, and disseminate a security policy that incorporates the following:
  - all PCI DSS requirements,
  - an annual process to identify threats and vulnerabilities with an annual formal risk assessment, and
  - an update of the process in the event of security environment changes.
- Develop daily operational security procedures consistent with requirements.
- Implement a formal security awareness program to make all employees aware of the importance of cardholder data security:
  - educate employees upon hire,
  - set up an annual education effort for all employees, and
  - require that employees acknowledge that they have read and understood the airport's security policy and procedures on an annual basis.

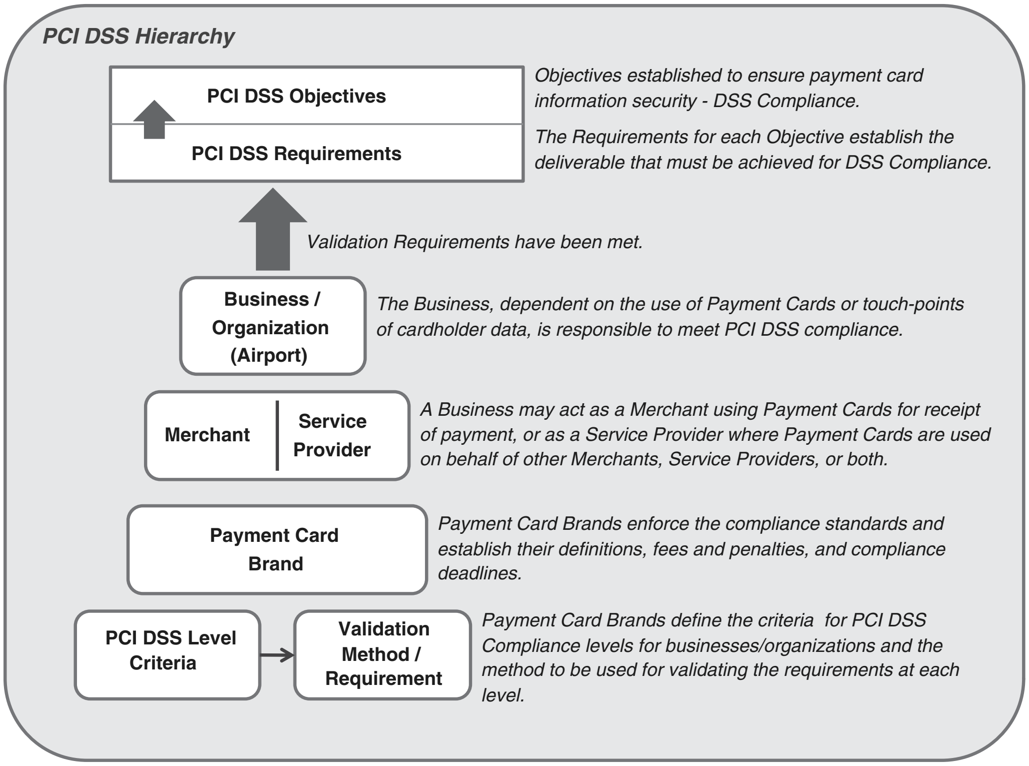

PCI DSS Hierarchy
PCI DSS Objectives
PCI DSS Requirements
Objectives established to ensure payment card information security - DSS Compliance.
The Requirements for each Objective establish the deliverable that must be achieved for DSS Compliance.
Validation Requirements have been met.
Business / Organization (Airport)
The Business, dependent on the use of Payment Cards or touch-points of cardholder data, is responsible to meet PCI DSS compliance.
Merchant
Service Provider
A Business may act as a Merchant using Payment Cards for receipt of payment, or as a Service Provider where Payment Cards are used on behalf of other Merchants, Service Providers, or both.
Payment Card Brand
Payment Card Brands enforce the compliance standards and establish their definitions, fees and penalties, and compliance deadlines.
PCI DSS Level Criteria
Validation Method / Requirement
Payment Card Brands define the criteria for PCI DSS Compliance levels for businesses/organizations and the method to be used for validating the requirements at each level.

Figure 5 Hierarchy of PCI DSS validations.

Understanding the PCI DSS requirements provides a first step to considering the impact on the airport business. However, the ability to achieve compliance still involves several factors. The business operation (merchant, service provider, or both), the card brands utilized by the business, and the criteria defined by the card brand applied to the business provide the basis for determining how the PCI DSS requirements will be validated. See Figure 5.

Whether a business is a merchant or a service provider, the use of a payment card or payment cardholder data in business operations requires a responsibility to meet PCI DSS compliance requirements. Each classification of business will then be subject to the criteria established by the payment card brand that is used by the business to further determine the validation requirements that must be followed to gain compliance.

In the sections below, it should be noted that many merchant classification levels and service provider classification levels indicate that a self-assessment can be conducted. This self-assessment is based on the number of transactions that are conducted annually. Additionally, the merchant or service provider can download the PCI SAQ from the PCI-Council website.

Merchant Classification—Level Criteria

Tables 2a–2e list by card brand the generally defined criteria for merchant-level assignment and the validation requirements at each level. Specific qualifications or conditions can be obtained from the source listed for each table.

Service Provider Classification—Level Criteria

Tables 3a–3e list by card brand the generally defined criteria for service provider-level assignment and the validation requirements at each level. Specific qualifications or conditions can be obtained from the source listed for each table or at the card brand website.

Compliance Deadlines

The deadlines for compliance validation are also subject to the discretion of the card brands and may even vary by merchant- or service provider-level or by the type of validation requirement. With the changing dynamics of deadline dates, there are no date requirements included in this document and deadlines should be verified through card brand PCI-knowledgeable representatives.

Table 2a Criteria for merchant-level assignment: Visa.

Level	Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region	1. Annual Report on Compliance (ROC) by Qualified Security Assessor (QSA) 2. Quarterly network scan by Approved Scanning Vendor (ASV) 3. Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	1. Annual Self-Assessment Questionnaire (SAQ) 2. Quarterly network scan by ASV 3. Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transaction annually	1. Annual SAQ 2. Quarterly network scan by ASV 3. Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	1. Annual SAQ recommended 2. Quarterly network scan by ASV if applicable 3. Compliance validation requirements set by Acquirer

SOURCE: Reference *8*.

Table 2b Criteria for merchant-level assignment: MasterCard.

Level	Criteria	Validation Requirements
1	Merchants that have suffered a hack or an attack that resulted in an account data compromise Any Merchant having greater than 6 million total combined MasterCard and Maestro transactions annually Any merchant meeting the Level 1 criteria of Visa Any merchant that MasterCard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system	1. Annual on-site review (qualified reviewer conditions must be met) 2. Quarterly network scan by Approved Scanning Vendor (ASV)
2	Any Merchant with greater than 1 million but less than or equal to 6 million total combined MasterCard and Maestro transactions annually	1. Annual on-site review at Merchant discretion (qualified reviewer conditions must be met)
	Any Merchant meeting the Level 2 criteria of Visa	2. Self Assessment required annually (qualified reviewer conditions must be met)
	Any Merchant meeting the Level 2 criteria of Visa	3. Quarterly network scan by ASV
3	Merchants processing greater than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to 1 million combined MasterCard and Maestro e-commerce transaction annually	1. Self Assessment required annually (qualified reviewer conditions must be met)
	Any merchant meeting the Level 3 criteria of Visa	2. Quarterly network scan by ASV
4	All other Merchants	1. Self Assessment required annually (qualified reviewer conditions must be met) 2. Quarterly network scan by ASV if applicable

SOURCE: Reference *9*.

Table 2c Criteria for merchant-level assignment: JCB.

Level	Criteria	Validation Requirements
1	Merchants processing over 1 million JCB transactions annually, or compromised merchants	1. Annual on-site review by Qualified Security Assessor (QSA) 2. Quarterly network scan by Approved Scanning Vendor (ASV)
2	Merchants processing less than 1 million JCB transactions annually	1. Annual Self-Assessment Questionnaire (SAQ) 2. Quarterly network scan by ASV

SOURCE: Reference *10*.

Table 2d Criteria for merchant-level assignment: AMEX.

Level	Criteria	Validation Requirements
1	Merchants processing over 2.5 million American Express transactions annually or any Merchant that American Express otherwise deems a Level 1	1. Annual Report on Compliance (ROC) by Qualified Security Assessor (QSA) 2. Quarterly network scan by Approved Scanning Vendor (ASV)
2	Merchants processing 50,000 to 2.5 million American Express transactions annually or any Merchant that American Express deems Level 2	1. Annual Self-Assessment Questionnaire (SAQ) 2. Quarterly network scan by ASV
3	Merchants processing less than 50,000 American Express transactions annually	1. Annual SAQ 2. Quarterly network scan by ASV

SOURCE: Reference *10*.

Table 2e Criteria for merchant-level assignment: Discover.

Level	Criteria	Validation Requirements
N/A	Merchants are currently not categorized into levels based on transaction volume. Discover takes a "risk based approach" for validating compliance	1. Quarterly Network Scan by ASV and one of the following: A. Annual on-site review by QSA-PCI DSS Assessment B. Annual Self Assessment Questionnaire

SOURCE: Reference *10*.

Table 3a Criteria for service provider-level assignment: Visa.

Level	Criteria	Validation Requirements
1	VisaNet processors or any service provider that stores, processes and/or transmits over 300,00 Visa transactions annually	1. Annual on-site PCI Data Security Assessment by Qualified Security Assessor (QSA) 2. Quarterly Network Scan by Approved Scanning Vendor (ASV)
2	Any service provider that stores, processes and/or transmits less than 300,000 Visa transactions annually	1. Annual PCI Self-Assessment Questionnaire 2. Quarterly network scan by ASV

SOURCE: Reference *11*.

Table 3b Criteria for service provider-level assignment: MasterCard.

Level	Criteria	Validation Requirements
1	All Third-Party Processors (TPPs) All Data Storage Entities (DSE) that store, transmit, or process greater than 300,000 total combined MasterCard and Maestro transactions annually	1. Annual on-site PCI Data Security Assessment by Qualified Security Assessor (QSA) 2. Quarterly network scan by Approved Scanning Vendor (ASV)
2	All DSEs that store, transmit, or process less than 300,000 total combined MasterCard and Maestro transactions annually	1. Annual PCI Self-Assessment Questionnaire 2. Quarterly network scan by Approved Scanning Vendor (ASV)

SOURCE: Reference *12*.

Table 3c Criteria for service provider-level assignment: JCB.

Level	Criteria	Validation Requirements
1	All Third-Party Processors (TPPs)	Undefined

SOURCE: Reference *13*.

Table 3d Criteria for service provider-level assignment: AMEX.

Level	Criteria	Validation Requirements
1	All Third-Party Processors (TPPs)	1. Annual on-site review by Qualified Security Assessor (QSA) 2. Quarterly network scan by Approved Scanning Vendor (ASV)

SOURCE: Reference *13*.

Table 3e Criteria for service provider-level assignment: Discover.

Level	Criteria	Validation Requirements
N/A	All Third-Party Processors (TPPs) and Payment Service Providers (PSPs)	1. Quarterly Network Scan by ASV and one of the following: A. Annual on-site review by QSA-PCI DSS Assessment B. Annual Self Assessment Questionnaire

SOURCE: Reference *13*.

Noncompliance Penalties

Fines may be imposed by the card brands when merchants or service providers do not meet the validation requirements by a stated deadline. Additionally, should cardholder data, owned within the airport business, be compromised, significant fines can be imposed by the card brands.

PCI AUDITS

Audit Preparation

Understanding Current Conditions

PCI DSS compliance is an intended way of doing business and not simply a one-time or annual event. The practices and requirements described in the previous section are items that may require new or improved operational processes and controls. A program would involve an ongoing process for monitoring, change control, maintenance, and administration.

An initial investigation as to where an airport stands in relation to classification (merchant, service provider, or both) is a required first step needed in order to assess the requirements that would apply. Additionally, an inventory assessment of assets focused on the areas that apply to PCI Data Security provides a foundation for investigation of security measures that may or may not be in place. The key for determining what should be included in the asset inventory is to identify the "touch-points" of cardholder data. Wherever cardholder data is stored, received, sent, or processed is the foundation for an inventory.

In any of the previous situations, the database, application(s), server(s), network(s), and gateway(s), including any back-up or mirrored systems, would need inclusion in the inventory. Assets need to include non-electronic locations as well. If there are file cabinets with cardholder information, or desk drawers that contain even handwritten cardholder information, these should be included in the asset inventory.

Having the asset inventory complete, a step-by-step application of the requirements to the assets will deliver "yes/no" responses as to whether the requirement is satisfied or not.

For example, a virtual private network (VPN) is in place and includes connection to a server with a database containing cardholder data. PCI DSS Requirement 1 states that the network must have a firewall configured to protect the data. The first question to answer is whether or not a firewall is in place on the VPN? If "yes," then is it configured in such a way that only authorized access to the data server and database can be achieved? If the answer to either of these questions is "no," then an action item can be established to implement the needed firewall. This process would be repeated for each asset within the PCI DSS environment owned by the airport.

Once the deficiencies have been identified, remediation efforts can begin by prioritizing the tasks necessary to make the "no" answers "yes" answers along with planned dates for completion. The PCI-Council provides a thorough checklist of items by requirement to help with detail considerations of a current environment assessment (*14*).

PCI Audit Approach

Using a PCI QAS for preliminary discussion on the airport's specific PCI DSS program strategy or approach is a good practice not only in preparing for an audit, but also for ensuring that a sound program is being developed for the long term. There are several PCI consulting firms promoting PCI compliance "readiness assessments" or "roadmaps" that can be used as an approach for dealing with the complexities of PCI DSS. The breadth of the program can include the beginning of assessing current conditions to remediation all the way through to audit and reporting.

Scheduled Audit Preparation

The business (merchant and/or service provider) should expect to invest time in preparation for a scheduled audit. The various preparation tasks should include:

- Documentation and Information—all information that could be utilized in presenting the various PCI DSS compliance aspects of the business should be collected and organized in a structure that will allow proper access and be readily available for an auditor or audit team. The information should be directly related to the intent to provide requirement compliance.
- Management and Staff—appropriate resources, including the manager and key staff members, should be identified prior to the audit and then presented at audit initiation. This effort will allow both the audit team and the organization resources to use time efficiently.

PCI DSS Qualified Roles

Depending on the PCI DSS compliance validation requirement, there are several authoritative or qualified roles that may be required to participate in an audit to achieve the validation.

Qualified Security Assessors

The PCI-Council qualifies companies as QSAs. Employees of QSA organizations have been certified by the PCI-Council to validate a business's compliance with and adherence to PCI DSS requirements. A QSA will work with an entity through audits and tests to identify missed requirements and to ensure that remediation achieves the desired compliance results. The PCI-Council has qualified more than 100 companies and has certified more than 1,500 assessors (*15*).

QSAs are generally required for validation purposes for merchants and/or service providers that are at the Level 1 category, and this is consistent across all card brands.

Approved Scanning Vendors

ASVs are organizations capable of performing vulnerability scans of a merchant's and/or service provider's Internet-facing system networks. More than 130 ASVs have been approved by the PCI-Council (*15*).

ASVs are required within multiple Merchant and/or Service Provider levels for requirements validation.

Self-Assessment Questionnaire

The SAQ serves merchants and service providers in multiple ways. One way is that it can be used to conduct a self-evaluation on an entity to assess where the organization is in regard to PCI DSS compliance requirements and to provide visibility as to where deficiencies may exist. The other service of the SAQ is for requirements validation mostly in the lower-transaction volume merchant and/or service provider levels.

Industry Certifications

The Society of Payment Security Professionals (SPSP) has developed two certification programs for the PCI. Individuals attaining certification are not included as qualified for PCI DSS compliance validation; however, they do provide businesses with another resource with high-level understanding of PCI knowledge. Some businesses include industry-certified resources as part of their financial or technology teams.

The certified PCI security manager (CPISM) identifies individuals who have gained expertise and have passed required tests in the areas of PCI structure, card structure and data, transaction processing, fraud statistics and trends, merchant risk analysis, laws and regulations, security programs, and third-party relationships (*16*).

The certified PCI security Auditor (CPISA) identifies individuals who have gained expertise and have passed required tests in the areas of information technology and networking, information security concepts, and auditing (*16*).

AIRPORT PCI

Understanding the PCI DSS and the requirements for compliance can create confusion in even the simplest of business operations, but airport operations can have several other variables that increase the complexity and add to the ambiguity. Between the network, databases and servers, applications, and the touch-points of cardholder data, the airport must understand who owns which piece of the PCI DSS responsibilities and set an approach or strategy not only to achieve compliance, but also to structure a program to ensure continued compliance.

This section examines the airport business processes that an airport must consider in developing a PCI DSS strategy. By taking a first step to understanding where the cardholder data "touch-points" exist, an airport can begin to organize the boundaries of their PCI DSS responsibilities.

Passenger-Initiated Processes

Booking/Reservations

A passenger today is capable of initiating reservations at off-airport venues where payment card data does not travel across any portion of the airport infrastructure and is not stored on airport systems and, therefore, would not be a PCI DSS responsibility of the airport. However, some on-site ticketing operations are conducted at the airport that, on the basis of the PCI DSS compliance requirements, would be an airport's responsibility. While ticketing functions may be handled at an airline-operated station on the airline-owned systems, investigation is required to determine if payment card data used at the station is transmitted to the airline connection using any portion of the airport's network. If such is the case, the airport would need to identify that situation as a touch-point and would need to apply PCI DSS security measures accordingly.

Since many booking and reservation processes can be accomplished using the Internet, an airport that provides Wi-Fi access to passengers, either as a free or paid service, would be required to address wireless network access points as a touch-point for inclusion in a PCI DSS program. However, in airports where Internet access is not provided, this situation would not be applicable.

Check-in

Passenger check-in may include multiple opportunities for using cardholder data. Passenger identification using cardholder data may be initiated with the use of a payment card. Additionally, actual payment transactions may be used for baggage fees (e.g., checked-bag, excess bags, and excess weight charges), flight upgrades for the passengers, seat charges, plus any other options presented to the passenger for purchase.

These functions may be conducted on passenger-facing airline-proprietary equipment or through common use self-service (CUSS) kiosks, as shown in Figure 6. Whether the check-in process is conducted in the airline-proprietary or common use scenario, the passenger could be using a payment card to initiate the check-in procedure. Based on the network configuration of the airport, if the cardholder data is transmitted across any portion of the airport-owned network, then a cardholder data touch-point should be identified.

Figure 6 Passenger check-in at a CUSS kiosk.

In addition to data transmission across the network, the use of payment card data for any processing within airport operations creates the need to address data security compliance. If the data is stored, even temporarily, in a database or if further processing is conducted on the data either prior to transmission or upon a receiving transmission, then a database touch-point can be acknowledged and the PCI DSS compliance requirements relating to secure systems, applications, and data access would need to be assessed.

Airlines engaged in business with the airport do not have an opportunity to choose a service provider for connectivity within the airline systems and are therefore in a "captive" environment. They must gain connectivity through an airport network and possibly through airport systems in which common use systems are employed. Airports must be in PCI DSS compliance and the proper level of due diligence employed to ensure the integrity of the airline customers' cardholder data and the tenant airline's public reputation as well. Part of the due diligence of an airline is to find secure providers. However, in a captive environment, this is not always possible and could impact the airlines' ability for PCI certification.

On-Airport Dwell Time Services

Depending on an airport's size and business model for tenants (non-passenger processing functions), there could be a vast array of POS functions being conducted through multiple businesses, both retail and service, in leased or rented spaces on the airport property. At every POS opportunity, if the business merchant accepts payment cards for purchases, the cardholder data needs to be protected to meet DSS compliance.

Where cardholder data is transmitted across any portion of an airport-owned network, that network and active infrastructure devices are required to meet the PCI DSS requirements. The key again is the cardholder data. In POS situations, the POS terminal may be in assessment scope depending on the ownership of the terminal (supplied by the airport, tenant contracts their own, etc.). The network used by the tenant to transmit the transaction is in the scope of the airport assessment if it is owned by the airport.

Airports that collect POS data from tenants for use in the airport business operation (tenant charges based on sales volume, percentage of sales paybacks, etc.) may also need to assess the data storage and processes in light of PCI DSS compliance. Any data collection that contains cardholder data extracted from the POS transactions would be required to undergo PCI DSS compliance requirements. In some instances, there could be hardcopy reports that are generated and shared between tenant and airport containing cardholder data, thereby generating the need for PCI DSS requirements relating to data protection.

In some airports, the airport and/or airline may charge for access to lounges, clubs, VIP membership services, and so on. The considerations described for airport tenants would be required to undergo the same scrutiny to uncover cardholder data touch-points that would need to be addressed as a part of the PCI DSS assessment.

A Wi-Fi service provided by airports to its passengers in either a fee-paid or free scenario is becoming more and more popular. Considering the fee-paid situation, the fee itself may be secured through a payment card transaction via the Internet. If the cardholder data is captured by an airport system, stored, or used for processing, then there is the obvious requirement to secure the data in regard to the DSS. The wireless access points, whether used through a pay for service or free service, will need to be investigated and assessed according to PCI compliance.

Arrival

Potentially, parking revenue control systems are a key element of an airport's revenue stream. In many cases, the collection of parking fees is conducted with the capability of using payment cards to reconcile the fee amount. Very similar to the other scenarios described, the set up of the network, the use of the cardholder data, and the processing methods employed for the payment transaction create an impact on the PCI DSS requirements the airport must address.

Tenant-Based Business Processes

In the course of standard business that takes place between on-site tenants and the airport, there are multiple transactions that may occur between the two. The method used for paying the appropriate fees to the airport are varied as well and may be unique based on the contractual arrangements.

The system used by the airport to conduct receivables may permit the use of payment cards and may or may not utilize cardholder data (business or personal) in conjunction with the payment transaction. The capture of the cardholder data, stored, processed, or transmitted to handle the business transaction, becomes the key to identifying another touch-point within the airport business operation that is expected to comply with PCI DSS requirements (Figure 7).

Figure 7 Tenants rely on airport compliance with PCI DSS requirements.

Transactions that could be included, depending on the airport business system model, are as follows:

- Lease payments,
- Rental payments,
- Utility payments,
- Service provider payments, and
- Penalties and fees.

Some airports store the cardholder data in an electronic format, such as in a spreadsheet or as hardcopy, such as notes in the tenants' files. It may seem logical to store this data for later use, such as with T-hangar rentals, lease payments, and others, but this storage is prohibited by PCI DSS.

Airport Operations Business Processes

Normal airport business requires payables that could also be susceptible to the PCI DSS should payment cards be utilized to initiate the payment transaction. Payments made using direct bank access (non-card brand debit cards, paper checks, etc.) would not be a PCI DSS issue from the airport perspective because there is no touch-point of payment card data being transmitted or processed.

Stored payment card data in the payables system would need to comply with PCI DSS requirements. Again there are many portions of the requirements that would be dependent on the configuration of the network; access capabilities to the data; how the data is processed and transmitted; and the security of the network, servers, and databases.

A key starting point for discovery of PCI DSS compliance is not unlike the other areas previously discussed. Where is payment card data stored and what are the touch-points of the data? The airport should be able to assess what databases store payment card data, what systems use that database, what servers house the database, what networks are used for data transmission, and so on.

Concerns

From an airport's perspective, PCI DSS compliance raises many questions and concerns, but clarification is not always readily available. Airports that have had some experience with PCI DSS programs, whether just starting or in progress, have discovered that even interpretation by the QSAs is subject to variations, and the validation requirements or remediation requirements could be more or less stringent depending on the QSAs' interpretations. What follows are some discussion points on these areas.

Scope of PCI DSS Compliance

Systems

The airport IT organization is heavily relied upon for a PCI DSS compliance program. One airport interviewed during the research emphasized that the inclusion of IT is instrumental for achieving successful results. Even though the airport director's sponsorship and enforcement is recommended, the IT organization will be expected to address not only current assessment data, but will probably also be required to accomplish the remediation efforts.

Purchased software may be considered "PCI ready" and should therefore meet the PCI DSS for payment application software. However, the installation and configuration of the software and/or the platform on which the system is implemented could create an "out of compliance" situation.

PCI DSS security requirements should be examined to ensure that compliance is met for any in-house developed software in production for any payment applications within the airport. There is a PA DSS established by the PCI-Council for developers of payment application systems, however, as long as the in-house developed software has not been sold to a third party, the PA DSS does not apply.

Airports responding to the research team interviews reported that the scope of systems in their current or planned PCI DSS compliance program included:

- Common use systems,
- Parking revenue control systems,
- Commercial vehicle management,
- Network,
- POS applications, and
- Any system involving payment card data.

Each airport must consider its business systems as unique and should investigate applications or systems in which payment card data is stored, processed, or transmitted, and include them in the program scope.

Platform

The platform used by the airport is not necessarily a stand-alone component in the PCI DSS scope, however, it potentially can have an impact on systems or networks with certain restrictions or functionality that a system must abide by in order to meet compliance requirements. A platform includes the operating system, computer architecture, and programming languages that are used for an application to run on. Remediation of non-compliance situations will require an updating of the system, hardware, and network as a part of the solution.

Network

Network configuration and segregation will be critical in determining required data security protection. The suggestion of one airport interviewee was to protect the data moving outward. Applying firewalls can be costly, but the security of the data during transmission will be extremely crucial for ensuring that the data remains protected during its time on the airport network.

Core Room

A core network room or server room where systems that hold cardholder data or where network administration/management is conducted and where cardholder data is transmitted, requires not only security of the systems and network access, but also security of physical access to the room itself. A physically secure location would include, minimally, the ability to monitor access and the ability to log the in and out activity of the room in addition to any actual network server access activity.

Resources

Attention to a PCI DSS compliance program can require extensive resources from the point of self-assessment through remediation, qualified assessment, and then ongoing maintenance and administration. Optionally, airports must determine, on the basis of their current resource allocations, whether they contract resources for each of the phases.

Smaller airports may find the resource requirements to engage in the PCI DSS daunting and will need to consider outsourcing a majority of the tasks, which could increase the cost of the program from the beginning. Even with this initial obstacle overcome, the need to have the resources required to comply with ongoing management and administration of the program may require outsourced arrangements as well. An airport respondent stated that there was a need to have one resource responsible for network security, however, the organization did not have a separation of duties to comply with that demand. Potentially, reorganization may be required. However, this could lead to the need for additional resources, which may conflict with budgets and staff size.

Requirements

The 12 requirements established for PCI DSS compliance apply to all businesses, organizations, or service providers for which payment card data is stored, processed, and transmitted. Airports question if there are any of the 12 requirements that do not apply to airports or that do not apply on the basis of the size of the airport.

The perspective of the card brand industry is that the 12 requirements are the 12 requirements and they apply throughout, regardless of the business type or situation. The size of the airport is not a a variable in determining the compliance expectations. The determining factors are:

- Does the airport operate as a merchant, service provider, or both?
- At what level within the merchant and/or service provider criteria does the airport operate? (This is based basically on the volume of transactions processed annually.)

Once the above questions are answered, the validation requirements, again, defined and enforced by the card brand, will then be known so that the airport can begin to develop the plan for meeting compliance.

Each requirement should then be investigated as it applies to the airport and the determination made as to what validation requirements will need to be met in order to meet compliance. As an example, a large airport providing wireless access to its passengers will be required to demonstrate security at the wireless access points, whereas a small airport that has no wireless network in place will not have to meet the same requirement. It is not the size of the airport, but the operation of the airport that is the determining factor.

Time Investment and Plan of Action

The time required to act on PCI DSS compliance is relative to the complexity of the program that needs to be implemented. According to the airports interviewed for this research, the time span ranged anywhere from 8 months to 5 years. Multiple airports responded that their time investment is estimated based on a target date in the future, out 1 to 2 years. As with many projects that extend over multiple years, unforeseen circumstances could create an impact on the schedule.

An airport can begin with an understanding of the tasks that should be considered when developing a time line for their PCI DSS program. These tasks can include:

Assessment of Current Environment—an assessment of the current airport environment sets the groundwork for determining what needs to be done. The assessment can include:

- Inventory of Documentation Available—what and how current is available documentation relating to network diagrams, office space diagrams, system and software inventory, database inventory (cardholder data), servers and server content.
- PCI DSS Scope—using the inventories, the cardholder data touch-points can be identified for decision on what is to be included in the PCI DSS compliance program.
- Identify Security Components—identify what security systems are in place for the network, database, or system access, as well as physical security conditions (room security).

Action Plan for Current Environment—on the basis of what is uncovered in the assessment phase, a plan of action will need to be developed. The plan of action will take into consideration priorities, resource requirements, other projects, and the cost considerations. One airport reported that they used the SAQ to determine the tasks to plan for. At this point, an airport would have the option to engage QSAs or consultants to analyze the current environment and to determine next steps, priorities, and time considerations.

Remediation Tasks—the time investment here could be extensive depending on the pre- and postaudit remediation tasks that have been identified. In some cases, airports have included the remediation tasks as part of existing or planned projects such as network upgrades or installations. System modifications or replacements are projects in and of themselves due to the rigor surrounding requirements gathering, design or procurement decisions, training, and implementation.

Audit—the audit time investment will be dependent on the level criteria of the airport. Preparation for the audit, contracting the auditor(s), scheduling the audit, and aligning resources for audit access and research/test execution will all be included in the time estimate. The required annual or quarterly ongoing tests should also be included in time budget planning.

Cost

Similar to the time investment, the costs associated with a PCI DSS compliance program are varied as well. While the interviewed airports reported a fairly low cost component, most were considering only the actual expense of hiring the qualified resources to conduct the validation requirements. However, in one case, an airport included the cost to replace a parking revenue control system that was required in order to become compliant. The need to replace or vastly overhaul a system in order to become compliant should be included in the cost considerations for the program. The program cost should encompass not only the cost of compliance, but the remediation cost as well.

It should not be surprising that costs are relative to the validation requirements that an airport may be required to address. The merchant- or service provider-level will have an impact on the program cost due to the stringency of the validation requirements and potentially due to the QSA interpretation of what the airport must do to achieve compliance. Also, the costs of the program may be spread across years depending on the deadlines imposed for the requirements. In some cases, an extreme, up-front outlay of cost may be required due to an impending deadline, when in other cases, the cost may be able to be budgeted over multiple quarters or years if the luxury exists that the deadline is further in the future.

Cost of Compliance

- Documented network diagrams and policies—depending on what documentation an airport currently has available, it may be a required to develop the documentation from scratch. Potentially, if documentation exists, the relativity to the actual current environment may require minor or significant updates. Either of these conditions will consume existing resources or require additional resources to accomplish.
- Resource costs—internal resource costs are sometimes "not counted" since the airport pays its employees regardless of the task assignment. However, the cost of internal resource should be counted because these resources may no longer be available for other tasks required in the operation. Additionally, resource consumption for training, both for trainers and trainees, can be extensive.
- Asset inventory—resource consumption will be required to identify the assets that are to be included in the scope of the PCI DSS program. As mentioned before, in addition to the network and network components, servers, software, and passenger-facing hardware (CUSS kiosks) are some of the assets to include. Any backup environment of the systems should be included in the inventory as well. The asset inventory should also include hardcopy data/reports that may contain cardholder data, which may be stored throughout the airport facility. These are assets that would require security in addition to the electronic data.
- Testing—the testing task is one that could include preliminary testing prior to the actual testing required by audits. This testing could uncover remediation necessities that can be addressed before scheduling audits.
- Assessments and Audits—the cost of contracting the appropriate qualified assessment companies or suppliers will be based on the validation requirements for the level of the airport. In some cases, businesses have hired or invested in in-house resources to become certified in the PCI industry in order to enable some of the validations to be met with internal resources. Additionally, costs should be captured for in-house resources that are devoted in part or full time to the test and validation process as well as foro the time these resources devote to the PCI auditors.

Cost of Remediation

- System modifications or replacements—depending on the findings of the systems within the scope of the PCI DSS, the need for major overhauls or potentially even replacement may be required. One area that was brought up by airports currently in PCI DSS programs was that of the parking revenue control system. These systems may have been in operation for an extended time and potentially have been in operation prior to many of the PCI DSS compliance requirements being formalized or to the deadlines imposed. The cost of building requirements, procuring a new system, testing, and implementing are not to be underestimated. If a system has been developed in-house and is going to be modified, the security requirements defined in the PCI DSS are in scope of the program.

- Network security implementations or enhancements—the cost considerations for network upgrades, firewall installation, encryption capabilities, and segregation will include resources, either in-house or contracted, in addition to network management and administration software. Additional hardware may also be required to bring resolution for meeting failed requirements.
- Physical access to rooms, file cabinets, and desks—to achieve compliance, it may be necessary to install locks or access systems to secure cardholder data. Depending on the system incorporated to meet compliance, the system could include key lock hardware and key control administration, a key card system with key card readers and locks with system administration for managing card distribution and security access maintenance. In some cases, depending on what an airport currently utilizes, an extension of an existing system may be required.
- Process and policy development—as modifications are made to systems, the processes required to manage the security may need to be developed or modified as well. Process changes may be required on the basis of new policies that need to be implemented. These tasks also require resources, and the cost should be applied to the remediation costs.
- Resource additions for ongoing policy, procedures, and administration—to ensure continued compliance, the remediation actions may require either a reallocation of current resources to take on the responsibilities of the new security procedures or possibly the addition of resources to manage the tasks. These resources may be secured through third-party vendors or through new hires.

PCI IN COMMON USE

Complex Environment

In airport environments, “common use” is a term used for equipment that is used by multiple air carriers to conduct the business of processing passengers. This equipment could be agent-facing, known as common use terminal equipment (CUTE) and now common use passenger processing systems (CUPPS), as well as passenger-facing, known as CUSS kiosks. While the overall focus of the equipment is a bit different from a technical perspective, the issues with respect to PCI between the agent-facing and passenger-facing common use entities are similar. This document will highlight where differences in the two types of processing occur.

All of the specifications, recommended practices, and processes are created as industry standards and are based on recommended practices that are published by IATA. The specifications generally describe the standards and interfaces that allow multiple airline applications to operate on a single platform and a common set of hardware. The working groups, which are responsible for the recommended practices, are currently investigating the impacts of PCI and how these systems can comply with PCI. The credit card industry, through this investigative activity, is becoming aware of the uniqueness of the airport/airline relationship and of the relationship between multiple merchants in a common use environment.

Uniqueness to Air Transport Industry

Common use creates a nexus between the airport, the airlines operating at that airport, and the vendors who provide common use solutions for common use practices. While many other IT systems that the airport manages and operates are primarily airport owned, or owned via contracts with vendors who supply the systems, common use adds the element of airlines operating on a common hardware platform. This common hardware platform allows multiple airlines to share IT equipment, but the IT equipment connects to the individual airline host systems through the use of network technology. Common use from a PCI perspective allows airlines to share common card reading equipment. This becomes the main challenge in the common use airport when considering the PCI-DSS.

Each stakeholder in this relationship—airport, airline, and vendor—has responsibility for PCI certification of the common use system. Airlines, as the merchants, are responsible for meeting merchant requirements of PCI DSS. Airports, as service providers, are at the very least responsible for meeting the service provider requirements of the PCI DSS. Vendors have a responsibility to provide PCI DSS ready equipment and services. With so many stakeholders, the path to PCI certification is far from straightforward.

The credit card brands have consistently stated that the air transport industry is unique when it comes to common use. In their experience, there has not been another example in which multiple merchants share the same credit card processing equipment. Because of this cross-utilization of card processing equipment, it is difficult to obtain PCI certification. Add to that the fact that passenger-facing self-service kiosks now use credit cards for payment transactions, as well as for identification purposes, the picture becomes even more complex. Ownership of equipment also complicates matters, as sometimes the common use equipment is owned by an airline, or an airline consortium, and other times it is owned by the airport operator. All of these stakeholders make a difficult situation, PCI compliance, even more difficult.

Varieties of Operational Models

To understand the complexities of common use and the PCI, it is necessary to understand some of the operating models that exist today. In all examples of common use, the one common denominator is that the equipment is capable of supporting multiple airline applications on a single set of hardware. Although the equipment is capable of this type of support, it is not necessarily always the case that the common use equipment is used by multiple airlines. However, in the cases where it is used by multiple airlines, the ownership models can vary as well. One ownership example is the common local user board model, or CLUB. In this model, the airlines own the common use equipment through a consortium of sorts, in which each airline has a vote and can determine the upgrade, replacement, and maintenance decisions of the equipment. Additionally, under the CLUB model, each airline can have its own maintenance contract with the common use solution provider. The airport itself may or may not be involved in a CLUB model.

Another ownership model is one in which the airport owns the common use equipment and provides it as a service to the airlines. Under this model, the airport maintains the contract with the solution provider. The airport is responsible for maintenance, upgrades, and support contracts for the system. The airlines are responsible for certifying their software on the selected platform for the airport.

Variations and complications can exist under both of the above-described models. One such complication occurs when the airport operator provides the network services from the demarcation point on the airport to the end devices, thus acting as a transport service, or a service provider. This type of model presents a unique challenge to the airlines when they are pursuing their PCI compliance, because if the airport is not able to obtain PCI certification, the airline does not have the opportunity to find another network provider.

Another complication is the governance, ownership, or management of the airport itself. Depending on the entity that owns and operates the airport, the PCI compliance that the airport is required to obtain can be confused by the greater organization's PCI compliance requirements. City-owned airports are a prime example of this. Under a city-owned airport, the airport operator may be required to meet the overall PCI DSS program of the city, rather than create a PCI DSS policy for the airport. This can further complicate the relationship between the airport and the airlines, as the entire city PCI DSS policy/program may not support external entities.

Airline operations introduce additional challenges. Today, airlines use credit card data for identity verification and data record location. This type of transaction does not require payment processing. Some of the credit card brands do not allow the use of credit card data for any other purposes than payment transactions. This means that the current practice of using the credit card for identification purposes is not acceptable in a PCI DSS world. The challenge for the airlines is that they could use hardware that would only return the identification data, and ignore the rest of the data on Track 1 of the magnetic stripe, but if they did that, and then required payment later in the transaction for additional services, the passenger would have to present their credit card a second time. There are many risks with this mode of operation, including confusing the passenger because he or she may think that the card was charged more than once.

Airport Considerations

This issue has become so important that IATA has created a separate PCI working group for common use. As this document is being written, this working group is attempting to define how to meet the PCI standards in a common use world. The first focus is on passenger self service, but the solution for passenger self service should be able to be applied to the agent-facing common use systems as well. It is not the intent of this document to prescribe a solution, but rather to identify the current state of the PCI DSS in the industry. The PCI working group will work toward a solution that meets the requirements of the card brands.

While not in use in the United States today, Chip and PIN systems present a unique challenge for common use. Unlike a magnetic stripe on a payment card where a signature is required to authorize the transaction, the Chip and PIN technology is based on an imbedded chip in the card. The information within the imbedded chip can only be activated by the associated PIN of the card owner. Even if the hardware today can be designed to process multiple merchants through multiple processing agents, the Chip and PIN solutions are pre-programmed in their chipsets to one specific processing agent. In a common use world, this would mean that all Chip and PIN transactions would have to go through one centralized processing agent. Since Chip and PIN is not in use in the United States today, it is very difficult to describe a solution for this issue.

The use of CUSS kiosks for passenger processing presents an additional variable to consider. In CUSS, the kiosk platform may also be supported by a vendor, so the vendor must certify the hardware platform, the air carrier must certify the check-in software, the airport might also have some software to certify depending on the implementation, and the airport might also be providing the network service. Such a scenario requires a collaborative effort between the airport, vendor, and airlines due to the mutual dependency to achieve PCI DSS compliance. Common use system vendors may consider their applications as PCI DSS compliant "ready," however, depending on how the system is installed and the infrastructure configured, the system may be rendered non-compliant. PCI compliant ready does not translate automatically as PCI DSS compliant.

Platform suppliers have started working with PCI QSAs to determine if their platforms can meet the PCI DSS. The QSAs meet with the platform suppliers, conduct audits, and identify any shortcomings with the platform supplier's solution. These shortcomings must be addressed before the audit can be completed. Once the audit is completed and passed, the platform cannot be identified as PCI compliant. This is due mainly to the fact that PCI compliance is dependent on the network, the software, and any applications that may interact with credit card data. Since the platforms are installed at airports with different network configurations, and with different airlines, it is impossible to provide a PCI-certified label to a common use platform. Some common use providers have taken to calling their tested products as PCI ready. This is meant to indicate that if they are installed on a proper network, and with proper applications, they would be able to pass PCI certification testing. While PCI ready is a nice start to identifying PCI compliancy, it is really not worth a lot in this environment simply because of all of the other variables involved.

Any PCI certification that involves common use will require coordination between all parties. The platform suppliers would do well to ensure that their platforms could pass PCI certification and therefore provide a PCI-ready platform. The airports will need to complete a PCI audit and remediate any shortcomings identified. And the airlines will need to complete their PCI audit and remediation in order to complete the PCI certification process. When all of these elements come together, the success, or failure, of a PCI certification process will be identified.

RESPONSIBILITY MATRIX

Basic Airport Responsibility

The responsibilities for PCI DSS security within an airport will vary from airport to airport depending on the operational methods and structure for payment card transactions for that specific airport. In general, the airport will need to ensure that data security standards are in place and that compliance can be assessed and validated for systems and applications, for the network(s), and for the physical locations of digital or hardcopy cardholder data.

Table 4 provides a guide for determining if an airport needs to address PCI DSS compliance at their facility. Depending on the answers to these questions, a minimal determination can be made as to whether an airport must indeed address PCI DSS compliance and initiate a program to meet those requirements as they apply to the airport's situation.

Table 4 addresses three categories of awareness for an airport to consider for PCI DSS compliance. The three categories of questions to be answered are "do you capture card data?" "do you process the data?" and "do you transmit the data?"

Table 4 PCI responsibility questions.

Description	Owned by	
Category 1: Card Data—Capture Method	**Airport?**	
CUSS Kiosk	Yes/No	"Yes" answer for any item = 'Y' for Category 1
POS Terminal	Yes/No	
Internet Website	Yes/No	
Application Input	Yes/No	
Manually Written	Yes/No	
Receipt from External System	Yes/No	
Category 2: Card Data—Processing	**Airport?**	
Card Data Stored (Database)	Yes/No	"Yes" answer for any item = 'Y' for Category 2
Card Data Processed (Application)	Yes/No	
Paper Stored (File Cabinets, Desk Drawers, etc.)	Yes/No	
Reporting Output	Yes/No	
Category 3: Card Data—Transmit	**Airport?**	
Local Area Network (LAN)	Yes/No	"Yes" answer for any item = 'Y' for Category 3
Wide Area Network (WAN)	Yes/No	
Private Network: Virtual Private Network (VPN) or Electronic Payments Network (EPN)	Yes/No	
Intranet	Yes/No	
Demilitarized Zone (DMZ)	Yes/No	

1. Are there any methods in the airport for which payment card data is captured?
   This category determines whether the airport owns the equipment or uses a method in which payment card data is captured. The methods listed need to be applied broadly in answering the question. For example, the Application Input question would apply to internal airport business applications, passenger-facing applications, web-enabled applications, and so on. If the answer to any of the methods is "Yes," then the answer for Category 1 should be "Yes."
2. Are there any areas in which payment card data is processed?
   Processing cardholder data includes situations in which the data, upon capture, is held temporarily and used to create other data (e.g., passenger identification number) or used for decisioning processes. Any "Yes" answers in this category renders the category as a "Yes" answer for the next step. Any physically handwritten processes or report output processes should not be overlooked.
3. Are there any processes in which payment card data is transmitted across the airport network or networks? Even if the airport does not store or process any payment card data electronically, if the payment card data travels across any portion of the airport-owned infrastructure, the network or networks involved must comply with data security standards. If the answer to any of the items is "Yes," then the answer for Category 3 is "Yes."

Table 5 provides an indication, on the basis of the answers to Table 4, as to where the airport must consider compliance initiatives. If an airport captures payment card data and does not store or process it, but does transmit the data, then network security compliance requirements would be the focus. Otherwise, an airport will need to consider all aspects in complying with the DSS. In the rare situation that an airport does not capture payment card data in any fashion, including handwritten or hardcopy, and, therefore, does not store or transmit payment card data, only then would the PCI DSS not apply.

NEXT STEPS—FUTURE RESEARCH

The research into the PCI DSS highlights several areas of recommended future research. These areas include:

1. *Clearly identify and delineate the roles and responsibilities of airlines, airports, and solution providers with respect to the PCI DSS.* It

Table 5 PCI responsibility result.

Cat. 1	Cat. 2	Cat. 3	PCI DSS Compliance Required?	PCI DSS Compliance Focus
Y	Y	N	Y	Systems, Network, and any Physical Storage
Y	N	Y	Y	Network
Y	Y	Y	Y	Systems, Network, and any Physical Storage
N	N	N	N	N/A

NOTE: Based on the responses to the three questions from Table 4, the combinations of answers above represent the four possible outcomes that result in the need (or lack thereof) for PCI DSS compliance and where the compliance effort will be required. Other combinations of answers would not be logical because data cannot be processed or transmitted if it is not captured, nor would data be captured if it isn't going to be processed or transmitted. (Cat. = category.)

is clear from the research that the parties in the PCI DSS value chain are not always aware of their PCI DSS responsibilities. In addition, it is clear that there is not a great understanding as to where the liability lies for each entity. The entities involved in PCI DSS applications, systems, and data transport need to be identified, and research is necessary to define the process by which the industry can identify delineations of responsibility.

2. *Further define the guidance for airports.* The PCI has created a list of six objectives. Further research is needed to present additional tips and guidance with respect to the 12 requirements of these objectives.
3. *Work with the PCI-Council to identify the aviation industry and solutions for the PCI DSS.* All research indicates that the PCI-Council does not yet understand the aviation industry. Some contacts within the payment card brands have stated that they understand the airlines, but not the airports, nor do they understand the role that airports play in the PCI DSS.
4. *Create a PCI handbook for airports.* PCI is more than the DSS, and airports need a more detailed document that helps them understand the nuances of the PCI. Understanding the differences between PCI DSS, PA DSS, and the other data standards is critical to the success of a PCI program. Additionally, an understanding of the auditing process, the difference between PCI ready, and PCI certified, and all of the other terminologies and documentation that are available for PCI is needed for airports to meet their requirements.
5. *Identify roles and responsibilities.* While the PCI DSS is mainly considered an IT problem, there are other disciplines and roles within the airport that have compliance responsibilities.
6. *Create a PCI guide for shared resources.* One of the unique elements in the aviation industry is the use of shared resources. This includes shared infrastructure, as well as shared credit card processing equipment running airline-specific applications (common use). Research needs to be conducted to create specific guidance for shared resources. IATA is currently overseeing a working group that is looking into this guidance specifically for CUSS, and ultimately for CUPPS, but other shared services are not currently included in this working group.

APPENDIX A—MAGNETIC STRIPE TRACK DATA

Table A.1 Magnetic stripe track data: Track 1.

	Developed by IATA	
Track 1 Element	**No. of Characters**	**Description**
Start Sentinel	1	"%" character indicating the beginning of the data in the next byte
Format Code	1	"B" for financial transactions
PAN	up to 19	account number (may include imbedded spaces as represented on card)
Separator	1	"^" character between PAN and next element
Name	up to 26	cardholder name
Separator	1	"^" character between Name and Additional Data
Expiration Date	4	YYMM
Service Code	3	code specifying acceptance and limitations
Discretionary Data	not to exceed total 76 characters of card (excluding sentinels)	elements defined by card brand for proprietary use (some of the PIN and Card Verification Values may be stored in this element)
End Sentinel	1	"?" character indicating the end of the card-holder data
LRC	1	longitudinal redundancy check character

SOURCE: Reference *17*.

Table A.2 Magnetic stripe track data: Track 2.

	Developed by ABA	
Track 2 Element	**No. of Characters**	**Description**
Start Sentinel	1	hexadecimal B ";" indicating the beginning of the data in the next byte
PAN	up to 19	account number (may include imbedded spaces as represented on card)
Separator	1	hexadecimal D "=" between PAN and next element
Expiration Date	4	YYMM
Service Code	3	code specifying acceptance and limitations
Discretionary Data	not to exceed total 37 characters of card (excluding sentinels)	elements defined by card brand for proprietary use (some of the PIN and Card Verification Values may be stored in this element)
End Sentinel	1	hexadecimal F "?" character indicating the end of the cardholder data
LRC	1	longitudinal redundancy check character

SOURCE: Reference *17*.

APPENDIX B—REFERENCES AND ADDITIONAL RESOURCES

REFERENCES

1. PCI Security Standards Council. *Payment Application Data Security Standard (PA-DSS) V1.2.* https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml. Accessed April, 2010.
2. Visa. *How It Works.* http://usa.visa.com/merchants/new_acceptance/how_it_works.html. Accessed March, 2010.
3. PCI Compliance Guide. *PCI FAQS—What Is the Definition of Merchant.* http://www.pcicomplianceguide.org/pcifaqs.php#13. Accessed April, 2010.
4. PCI Compliance Guide. *PCI FAQS—What Constitutes a Service Provider.* http://www.pcicomplianceguide.org/pcifaqs.php#13. Accessed April, 2010.
5. DED Limited. *Magnetic Stripe Card Standards.*http://www.ded.co.uk/magnetic-stripe-card-standards/. Accessed April, 2010.
6. PCI Security Standards Council. *Navigating PCI DSS, Understanding the Intent of Requirements.* https://www.pcisecuritystandards.org/pdfs/navigating_pci_dss_v1-1.pdf. Accessed March, 2010.
7. PCI Security Standards Council. *Glossary, Abbreviations and Acronyms.* https://www.pcisecuritystandards.org/security_standards/glossary.shtml#c. Accessed March, 2010.
8. Visa. *Merchants.* http://usa.visa.com/merchants/risk_management/cisp_merchants.html. Accessed April, 2010.
9. MasterCard. *Merchant Levels Defined.* http://www.mastercard.com/us/sdp/merchants/merchant_levels.html. Accessed April, 2010.
10. NDB Advisory. *Important PCI Compliance Information for Merchants.* http://www.pciassessment.org/merchants.php#bookmark-3. Accessed April, 2010.
11. Visa. *Service Providers.* http://usa.visa.com/merchants/risk_management/cisp_service_providers.html. Accessed April, 2010.
12. MasterCard. *Service Provider Levels Defined.* http://www.mastercard.com/us/sdp/serviceproviders/serviceprovider_levels.html. Accessed April, 2010.
13. NDB Advisory. *Important PCI Compliance Information for Service Providers.* http://www.pciassessment.org/service-providers.php. Accessed April, 2010.
14. PCI Security Standards Council. *Security Audit Procedures, Version 1.1.* https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf. Accessed April, 2010.
15. PCI Security Standards Council. *Qualified Security Assessors (QSAs)/Approved Scanning Vendors (ASVs).* https://www.pcisecuritystandards.org/qsa_asv/index.shtml. Accessed April, 2010.
16. SPSP Society of Payment Security Professionals. *CPISM.* https://www.paymentsecuritypros.com/CPISM/. Accessed April, 2010.
17. Magtek. *Brochures—Magnetic Stripe Card Standards.* http://www.magtek.com/documentation/public/99800004-1.03.pdf. Accessed April, 2010.

ADDITIONAL RESOURCES

American Express (card brand) website: https://www209.americanexpress.com.

American Express. American Express Data Security Operating Policy for U.S. Merchants. https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US.pdf.

American Express Data Security Home. Data Security for Merchants. https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home&ln=en&frm=US.

ARINC. ARINC's PCI-DSS Adventure. Presented at ACI BITCOM, Austin, Tex., Oct., 2009. http://www.aci-na.org/static/entransit/pci_margerison.pdf.

Barich, Inc. The Future of Airport Information Technology. Presented at ACI-NA Airport Board Members and Commissioners Conference, Chicago, Ill., April, 2009. http://www.aci-na.org/static/entransit/8-TheFutureOfAirportInformationTech-FBarich.pdf.

Coalfire Systems. *PCI Compliance: "Just the Facts."* Presented at ACI-NA Conference, Seattle, Wash., April, 2009. www.aci-na.org/about/resolveuid/2b2f756874a8dd06be8dca0163245f9c

The Compliance Authority website: http://www.thecomplianceauthority.com/pci-compliance-deadlines.php

CompliancesForum website: http://www.compliancesforum.com/download-pci-dss-audit-questions-and-checklist

Discover (card brand) website: http://www.discovernetwork.com/fraudsecurity/disc.html.

Discover Information Security and Compliance. http://www.discovernetwork.com/fraudsecurity/disc.html

Element website: http://www.elementps.com/merchants/pci-dss/compliance-level/.

GFI. PCI DSS Made Easy. http://www.gfi.com/whitepapers/pci-dss-made-easy.pdf.

GFI.com Whitepapers: http://www.gfi.com/whitepapers/pci-dss-made-easy.pdf.

IATA Payment Card Industry Data Security Standards. http://www.iata.org/whatwedo/finance/creditcard/pci-dss.htm.

IT Compliance Institute (ITCi). *IT Audit Checklist: Payment Card Industry (PCI).* http://download.101com.com/pub/itci/Files/ITCi_ITACL-PCI_0321-Lb.pdf.

JCB Data Security Program. http://www.jcb-global.com/english/jdsp/index.html.

ManageEngine website: http://www.manageengine.com/products/security-manager/pci-dss-compliance-checklist.html.

MasterCard (card brand) website: http://www.mastercard.com.

Mastercard. Security Rules and Procedures-Merchant Edition. http://www.mastercard.com/us/merchant/resources/downloads.html.

Motorola Helps Customers with PCI Solutions. http://www.motorola.com.

NDB Advisory website. http://www.pciassessment.org/ndb-advisory.php.

PCI Compliance Guide. http://www.pcicomplianceguide.org/pcifaqs.php.

PCI DSS and MasterCard Site Data Protection Program. http://www.mastercard.com/us/merchant/security/sdp_program.htmlAmerican Express Data.

PCI FAQS and Myths. http://www.pcicomplianceguide.org.

PCI Security Standards Council, LLC website: https://www.pcisecuritystandards.org.

PCI Security Standards Council, LLC. Navigating PCI DSS. https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf

PCI Security Standards Council, LLC. PCI—Glossary of Terms, Abbreviations, and Acronyms. https://www.pcisecuritystandards.org/pdfs/pci_dss_glossary.pdf

PCI Security Standards Council, LLC. PCI Quick Reference Guide. https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf.

PCI Security Standards Council, LLC. PCI DSS 1.2 FAQs. https://www.pcisecuritystandards.org/pdfs/pci_dss_1.2_faqs.pdf.

PCI Security Standards Council, LLC. Summary of Changes from PCI DSS Version 1.1 to 1.2. https://www.pcisecuritystandards.org/pdfs/pci_dss_summary_of_changes_v1-2.pdf.

The following are downloads available on the PCI Security Standards Council website in the Attestation of Compliance section: https://www.pcisecuritystandards.org/saq/index.shtml:

Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire Instructions and Guidelines.

Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire A and Attestation of Compliance.

Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire B and Attestation of Compliance.

Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire C and Attestation of Compliance.

Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire D and Attestation of Compliance.

QUALYS. *PCI for Dummies.* http://www.qualys.com/forms/ebook/pcifordummies/ttp://www.qualys.com/forms/ebook/pcifordummies/.

SearchMidMarketSecurity.com: http://searchmidmarketsecurity.techtarget.com/news/article/0,289142,sid198_gci1359064,00.html.

SITA. Common Use Systems and PCI Compliance. Presented atACI-NA Conference, Austin, Tex., Oct., 2009.

Society of Payment Security Professionals website: https://www.paymentsecuritypros.com/.

Trustwave website: https://www.trustwave.com/pciDataSecurityStandard.php

Visa. Cardholder Information Security Program. http://usa.visa.com/merchants/risk_management/cisp.html.

APPENDIX C—GLOSSARY OF TERMS

ABA—American Bankers Association.

Acquirer—bankcard (Visa, MasterCard, etc.) member that receives bankcard transactions from a merchant.

American Express (AMEX)—payment card issuer brand.

Application—purchased, in-house developed, or customized software designed for business use by internal users or passenger/customer use.

Asset—hardware, software, or other items used in the storage, processing, or transmission of payment card data.

ASV—approved scanning vendor.

Authorization—granted to an individual for access rights to information, applications, administration, or management purposes.

Backup—redundant or duplicate data intended for archival or restoration purposes.

Card Brand—financial organization issuing a payment card.

Cardholder Data—Primary account number plus the cardholder name, and/or card expiration date, and/or service code.

Card Validation Code—data element encoded within the magnetic stripe of a payment card, used to protect the integrity of the card data. Also known as:

- CVC: card validation code (MasterCard)
- CVV: card verification value (Visa and Discover)
- CAV: card authentication value (JCB)
- CSC: card security code (American Express)

CLUB—common local user board.

CPISA—certified payment card industry security advisor.

CPISM—certified payment card industry security manager.

CUPPS—common use passenger processing system.

CUSS—common use self service (IATA recommended practice for). Refers to the airline- and airport-provided check-in units travelers can use, often independently, for managing their travel check-in process. Often deployed in kiosk form, but not necessarily.

CUTE—common use terminal equipment.

DSE—data storage entities.

DMZ—demilitarized zone. A network layer positioned for security between a private and public network.

Encryption—data conversion technique that renders data unreadable except to authorized data receiver using the conversion key.

EPN—electronic payments network.

IATA—International Air Transportation Association.

IPSEC—Internet protocol security.

ISO—International Organization for Standardization.

IT—information technology.

LAN—local area network.

LRC—longitudinal redundancy character.

Magnetic Stripe Data—data encoded within specified formats (tracks) for the authorization of transactions for payment or identification purposes.

Network Scan—network tool capable of remotely checking merchant or service provider systems for potential privacy vulnerabilities.

PAN—primary account number. Payment card identification number linking cardholder to a specific account.

Payment Cardholder—authorized user of a payment card.

PA DSS—payment application data security standard.

PCI DSS—payment card industry (PCI) data security standard (DSS). The standards for compliance for payment card data protection that merchants, service providers, and organizations using payment cards in the operation of the business must abide by and attest compliance with.

PCI-Council—PCI Security Standards Council. A collaboration between Visa, MasterCard, Discover, American Express, and JCB International to create common industry security requirements.

PIN—personal identification number. Number assigned, generally at discretion of cardholder, to authorize use of payment card.

POS—point of sale.

Printed CVC—three- or four-digit code printed on the payment card for unique identification of the card. Also known as:

- CID: card identification number (American Express and Discover)
- CVV2: card verification value 2 (Visa)
- CAV2: card authentication value 2 (JCB)
- CVC2: card validation code 2 (MasterCard)

PSP—payment service provider.

PVKI—PIN verification key indicator.

PVV—PIN verification value. Encoded data on magnetic stripe of payment card.

QSA—qualified security assessor.

SAQ—self-assessment questionnaire.

Service Code—number on the magnetic-stripe data Track 1 and Track 2 that specifies acceptance and limitations for a read transaction.

Service Provider—any business that processes, stores, or transmits cardholder data on behalf of a merchant, other service providers, or any entity where cardholder data is used.

SPSP—Society of Payment Security Professionals.

SSL—secure socket layer.

SSU—self-service unit. A synonym for CUSS, used as a means of differentiating the housing of the hardware device from the generic term "kiosk," typically associated with CUSS, permitting more descriptive application of the hardware in dual-head counter configurations, imbedded counter configurations, and freestanding configurations. The use of SSU also permits specific definition of hardware that displays all airlines on the start page versus those of a specific airline in an allocated ticket counter scenario.

TLS—transport layer security.

TPP—third-party processor.

Transaction Data—cardholder data involved in a process (electronic or manual).

VPN—virtual private network.

WAN—wide area network.

Wi-Fi—wireless fidelity.

TRB

Transportation Research Board
500 Fifth Street, NW
Washington, DC 20001

Subscriber Categories: Aviation • Administration and Management • Data and Information Technology

ISBN 978-0-309-15502-1

90000

9 780309 155021

These digests are issued in order to increase awareness of research results emanating from projects in the Cooperative Research Programs (CRP). Persons wanting to pursue the project subject matter in greater depth should contact the CRP Staff, Transportation Research Board of the National Academies, 500 Fifth Street, NW, Washington, DC 20001.